Information Security Governance Manager
Job Description

JOB INFORMATION

Job Code:	166045
Job Title:	Information Security Governance Manager
FLSA Status:	Exempt
Supervisory:	
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	5 Manager

JOB SUMMARY

Responsible for owning, defining, and delivering infrastructure security governance across the Information Security Office, managing an enterprise Data Loss Prevention Program (DLP), and ensuring that governance processes are in place to maintain DLP controls. Assists in external and internal audits, ensures overall adherence to policy standards, oversees the Security Awareness program, and facilitates the highest level of compliance through assessment, remediation and escalation as necessary. Actively contributes to the security management team by managing, leading, and developing the team capability and customer impact, and works with IT internal support teams as well as external clients within the university to prove the highest standards of support relative to information and security governance practices. Utilizes the risk assessment process to educate asset and process owners on information security risks, risk management, and remediation options.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	X	Bachelor's degree		

Additional Education

Check here if experience may substitute for some of the above education.

X	Combined experience/education as substitute for minimum education

Work Experience

Req	*Pref*	*Work Experience*	*Experience Level*	
X		7 years		
	X	10 years		

Additional Work Experience

Check here if education may substitute for some of the above work experience.

	Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		An in-depth understanding of information security, security policies, account security policies and standards for logical and physical security implementations.
X		A basic knowledge of Regulatory Compliance as it affects the relevant industry.
X		A good understanding of the information security control measures as defined in ISO-17799.
X		A working knowledge of risk assessment as it is applied to information security.
X		The ability to perform, manage and run information security audits.
X		A sound understanding of security architecture and risk framework principles and concepts.
X		Demonstrable experience in running a comprehensive security awareness program.
X		Experience in a Federated or decentralized organization.
	X	Technical and Functional experience in domain of Governance, Enterprise Risk Management and Regulatory Compliance.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		CISSP, CISA, CISM, GSEC, CRISC, or related certification(s)

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Serves as a Subject-Matter Expert (SME) on the organization's strategy for the information security critical processes and associated tools, ensures the process aligns to regulatory, statutory and industry requirements and university policy and data classification. Recommends programmatic and technical direction with a high degree of independence in matters relating to the investigation, impact and analysis of decisions regarding cyber security risk.				
Develops, operates and manages comprehensive Information Security strategies, standards, policies and programs to assess, prioritize and mitigate business risk Leads the review and formal approval process for Policy updates. Coordinates updates to the Information Security Standards. Ensures Information Security Policy and Standard documents meet or exceed industry standards, compliance requirements and customer/client expectations.				
Assesses and manages the adequacy of the mitigation and remediation plans of known cyber security vulnerabilities and threats, aligning with the Information Security Governance & Risk Management (ISGRM) risk framework and processes.				
Owns, defines, leads and delivers information security governance across technologies, departments and data assets. Ensures any risk is identified, articulated and escalated through standard governance, mitigated and communicated to all stakeholders.				
Facilitates communication and execution of enterprise-wide information security programs and a comprehensive, multi-pronged security awareness training program. Provides regular guidance and advocacy for best practices for information security.				
Defines and executes an annual risk assessment plan, and obtains plan sign-off from key stakeholders across the university. Shows key milestones, metrics, KPIs, associated budget and resource impacts to continue an effective risk management program. Create and maintain an agreed upon Risk Appetite and Key Risk Indicators (KRIs) in line with the ISGRM Risk Framework.				
Manages design and implementation of an enterprise Data Loss Prevention Program (DLP). Ensures governance processes are in place to maintain DLP controls across the enterprise. Ensures that DLP controls manage risk in the changing threat landscape, meet business needs and client expectations, and regulatory expectations. Facilitates business rule reviews, threshold setting, and exception management.				
Engages in preparation of and participates in external and internal compliance audits (PCI DSS, HIPAA, NIST, ISO 27001:2013, etc.). Supports overall validation of				

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
adherence to policy and standards through control evaluation. Ensures compliance through assessment, remediation and escalation.				
Utilizes the risk assessment process to educate asset and process owners on information security risks, risk management and appropriate remediation options. Manages the risk acceptance process to ensure the implications of risk acceptance are understood, risks are accepted at the correct level within the organization, and risk acceptances are tracked and reported on throughout their lifecycle. Manages the risk exception process and regular review.				
Manages and maintains a risk reporting framework for management teams and governance committees. Defines and manages the Key Performance Indicators (KPIs) to assure effectiveness and compliance across processes and process owners.				
Maintains awareness and knowledge of current changes within legal, regulatory, and technology environments which may affect operations. Ensures senior management and staff are informed of any changes and updates in a timely manner. Establishes and maintains appropriate network of professional contacts. Maintains membership in appropriate professional organizations and publications. Attends meetings, seminars and conferences and maintains continuity of any required or desirable certifications, if applicable.				

Other Requirements

Essential:	*Emergency Response/Recovery*	*Essential:*	*Mandated Reporter*
	In the event of an emergency, the employee holding this position is required to "report to duty" in accordance with the university's Emergency Operations Plan and/or the employee's department's emergency response and/or recovery plans. Familiarity with those plans and regular training to implement those plans is required. During or immediately following an emergency, the employee will be notified to assist in the emergency response efforts, and mobilize other staff members if needed.		A mandated reporter who in his or her professional capacity has knowledge of, or reasonably suspects a person who is under the age of 18 years, elderly, or a dependent adult has been the victim of abuse or neglect must report the suspected incident. The reporter must contact a designated agency immediately or as soon as practically possible by telephone or in writing within 36 hours. By virtue of the associated job duties, this position qualifies as a mandated reporter as required by state law and USC's policy at: https://policy.usc.edu/mandated-reporters/

Campus Security Authority (CSA)	*Essential:*
By virtue of the associated job duties, this position qualifies as a Campus Security Authority as required by law and USC's policy at: https://dps.usc.edu/alerts/clery/	No

ACKNOWLEDGMENTS

The above statements reflect the essential and non-essential functions as necessary to describe the principle contents of the job. They are not intended to be a complete statement of all work requirements or duties that may be required of the position. I understand that I may be asked to perform other duties as assigned. USC reserves the right to add or change duties at any time.

The University of Southern California is an Equal Opportunity Employer. USC prohibits discrimination on any basis protected under federal, state, or local law, regulation, or ordinance or university policies. All employment decisions are based on individual qualifications and business need.

I acknowledge receipt of this job description and its associated physical requirements. I have read and understand the job description and job requirements and agree to abide by their contents. I realize that duties may be requested of me that are not specifically stated herein. I understand that I will be expected to adjust to potential fluctuations in work volume. I understand that, if I have any questions about the essential functions or expectations of my position, my supervisor and/or HR partner are available to discuss them with me.

Print Employee Name	Signature	Date

Print Manager Name Signature Date

This job description describes the general nature and level of work required by the position. It is not intended to be an all-inclusive list of qualifications, skills,
duties, responsibilities or working conditions of the job. The job description is subject to change with or without notice, and Management reserves the right to add, modify or remove any qualification or duty. Nothing in this job description changes the existing at-will employment relationship between the university and the employee occupying the position.